Colorado Privacy Act (CPA) Readiness Record

The Lucid readiness record is a quick tool to ascertain the CPA maturity of your business.

This easy questionnaire is designed to start to collect information to record, measure and prioritise privacy work.

For more information on how to assess and remediate your current Privacy Program, please contact Lucid Privacy directly.

Jurisdiction[1]	
Does your organization conduct business in the state of Colorado or with people (or devices) in Colorado?	
Does your organization collect consumers' personal data? (including any unique identifiers) If yes, list identifiers	
Does your organization control or process the personal data of 100,000 or more Colorado consumers in a year? (including unique website visitors)	
Does your organization derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers? (including 3rd party advertising services monetizing website visitor data)	
Exemptions: Your organization is not; 1. a Colorado state or local governing body, 2. a state institution of higher education, 3. subject to GLBA, HIPAA, FERPA, or exclusively using employment data. [Note; nonprofits are not exempt under the CPA]	

[1] CPA § 6-1-1304.

Governance[2]	
Is there a Privacy (Data Governance) Committee?	
Are roles and responsibilities for privacy management assigned?	
How do senior executives and leadership teams engage with matters relating to privacy and privacy risk?	
Policies	
List all relevant organizational policies relating to privacy management, eg. website privacy policy, record of processing activities, data protection policy, information security/breach policy, retention policy.	
Individual Rights	
Provide details of your individual rights management processes. (eg; access/deletion/modification/opt-out) Do you provide individuals with the following rights? • right to know; • right to access; • right to correct; • right to delete; • right to opt out of sale; • right to opt out of targeted advertising; • right to opt in to the processing	

[2] The provisions of this section "Governance" are not requirements under the law, but best practices in order to comply with other requirements.

• of sensitive information (detailed further below); and • right to non-discrimination for exercising these rights.	
Provide details of your organization's approach to opt outs of the 'sale' of personal data.[3] (eg; direct mail lists, not third party cookies)	
Provide details of your organization's ability to honor opt-out preference signals (aka; 'global privacy controls').[4]	
Provide details of your organization's approach to consumer opt outs of targeted advertising.[5] (eg; third party advertising cookies or social media matching)	
Provide details of your organization's approach to obtain consumer opt in consent for the processing of sensitive personal data.[6] CPA defines sensitive personal data as: (1)data collected from a known child; (2) racial or ethnic origin; (3) religious beliefs; (4) sexual orientation; (5) information regarding an individual's sex life; (6) citizenship or immigration status; (7) mental or physical health diagnosis and conditions; (8) genetic or biometric data for the purpose of identifying an individual.[7] (eg; identifiable/tagged photos)	
Provide details of your organization's approach to consumers opt outs of automated profiling that may lead to a	

[3] § 6-1-1306(1)(a)(B).
[4] § 6-1-1306(1)(a)(IV).
[5] § 6-1-1306(1)(a)(A).
[6] § 6-1-1308(7).
[7] § 6-1-1303(24).

'significant decision'.[8]	
Provide details of your individual rights management processes relating specifically to processing data of children.[9] (if relevant)	
Provide an overview of the individual rights identity verification process.[10] (eg; what is needed in order to grant access to, or delete, their personal data)	
Provide an overview of the consumer rights appeal process for denial of consumer request.[11]	
Privacy Notice	
Provide a link to your public-facing Privacy Notice. Under CPA, a privacy notice must include: ● the categories of personal data collected or processed by the controller or a processor; ● the purposes for which the categories of personal data are processed; ● how and where consumers may exercise the rights[12] including the controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request; ● the categories of personal data that the controller shares with third parties, if any; and ● the categories of third parties, if any, with whom the controller	

[8] § 6-1-1306(1)(a)(C).
[9] § 6-1-1308(7).
[10] § 6-1-1306(1).
[11] § 6-1-1306(2)(b).
[12] pursuant to § 6-1-1306.

shares personal data.[13] If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.[14]	
Data Mapping[15]	
Do you have an inventory of, or record of personal information and associated processing activities?	
Do you have an information asset register?	
Training	
Provide details of your privacy training programme.[16]	
Data Minimization	
Does your organization only collect personal data that is "adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed"?[17]	
Secondary Use	

[13] § 6-1-1308(a).
[14] § 6-1-1308(b).
[15] The provisions of this section "Data Mapping" are not a requirement under the law, but a best practice in order to comply with other requirements.
[16] The CPA does not require employee privacy training but is a best practice in order to comply with other requirements.
[17] § 6-1-1308(3).

Does your organization only process personal data that is reasonably necessary or compatible with the purpose(s) specified in the privacy policy and not process personal data for any secondary use?[18]	
Retention[19]	
Do you have in place a classification and retention policy and retention schedule?	
Security[20]	
Do you have an information security policy?	
Describe your organization's arrangements for managing information security and associated risks.	
Risk	
Do you have an information risk policy in place?[21]	
Do you have a privacy risk register?[22]	

[18] § 6-1-1308(4).
[19] The provisions of this section "Retention" are not a requirement under the law, but a best practice in order to comply with other requirements.
[20] § 6-1-1305(4). CPA requires, "Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures."
[21] This is not a requirement under the law, but a best practice in order to comply with other requirements.
[22] This is not a requirement under the law, but a best practice in order to comply with other requirements.

How is privacy risk communicated to senior management and throughout the organization?[23]	
Have you conducted data protection assessments for all processing that presents a heightened risk of harm to consumers, including processing personal data for targeted advertising or sales, certain types of profiling, and processing sensitive data?[24]	
Data Breach	
Do you have a data breach/incident response policy in place?[25]	
Vendor/Contract Management	
Do you have a policy governing processing of personal information by third parties/vendors?[26]	
Have you mapped out all vendors processing personal information?[27]	
Are Data Processing Agreements/contractual terms in place	

[23] This is not a requirement under the law, but a best practice in order to comply with other requirements.

[24] § 6-1-1309. Controllers must conduct a 'data protection assessment' when there is a heightened risk of harm to consumers, including but not limited to: (1) Targeted advertising; (2) Sales of personal data; (3) Processing personal data for profiling which creates certain risks for consumers (including unfair or deceptive treat; unlawful disparate treatment; or financial, physical; and other risks); and (4) Processing sensitive data.

[25] This is not a requirement under CTDPA, but under Colorado's data breach notification statute Colo. Rev. Stat. § 6-1-716.

[26] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 23).

[27] this is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 23).

with all processors?[28]	
Do you conduct privacy specific vendor due diligence before engaging vendors?[29]	

[28] 6-1-1305((5).
[29] This is not a requirement under the law, but a best practice in order to comply with other requirements.